

## UNITED STATES DISTRICT COURT

for the  
District of South DakotaIn the Matter of the Search of:  
Google Cybertip #62781662

Case No. 5:20-mj-69

## APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

SEE "ATTACHMENT A", which is attached to and incorporated in this Application and Affidavit, located in the District of South Dakota, there is now concealed *(identify the person or describe the property to be seized)*:

SEE "ATTACHMENT B", which is attached to and incorporated in this Application and Affidavit

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☐ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

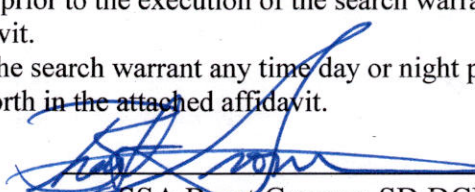
The search is related to a violation of:

*Code Section*  
 18 U.S.C. §§ 2251, 2252, and 2252A

*Offense Description*  
 Possession, Receipt, Distribution, and Production of Child Pornography

The application is based on these facts:

- ☒ Continued on the attached affidavit, which is incorporated by reference.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.  
☐ Your applicant requests that no notice be given prior to the execution of the search warrant, i.e., "no knock", the basis of which is set forth in the attached affidavit.  
☐ Your applicant requests authorization to serve the search warrant any time day or night pursuant to Fed. R. Crim. P. 41(e)(2)(A)(ii), the basis of which is set forth in the attached affidavit.

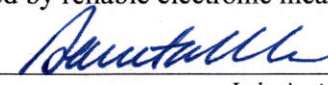
  
 SSA Brent Gromer, SD DCI & FBI TFO

Sworn to before me and: ☒ signed in my presence.

☐ submitted, attested to, and acknowledged by reliable electronic means.

Date: 3-23-2020

City and state: Rapid City, SD

  
*Judge's signature*

Daneta Wollmann, U.S. Magistrate

*Printed name and title*

UNITED STATES DISTRICT COURT  
DISTRICT OF SOUTH DAKOTA  
WESTERN DISTRICT

---

IN THE MATTER OF THE SEARCH OF:

CR 5:20-mj-69

Google Cybertip #62781662

**AFFIDAVIT IN SUPPORT OF  
SEARCH WARRANT  
APPLICATION**

---

State of South Dakota     )  
  ) ss  
County of Pennington     )

INTRODUCTION AND AGENT BACKGROUND

I, Brent Gromer, being duly sworn, state as follows:

1. I am a Supervisory Special Agent with the South Dakota Division of Criminal Investigation. I have been employed as a Law Enforcement Officer in the State of South Dakota for over 23 years. In 2018, I became a Task Force Officer (TFO) for the Federal Bureau of Investigation. I have been involved in numerous investigations into all manner of crime. I have received training in Search and Seizure from the South Dakota Attorney General's Office, United States Attorney's Office, the United States Drug Enforcement Administration, Federal Bureau of Investigation and other private training organizations. I have personally prepared numerous affidavits in support of request for search warrant. State and Federal courts have granted search warrants based on those affidavits that have withstood suppression efforts.

2. Since June of 2010, I have been assigned to the Internet Crimes Against Children (ICAC) Task Force in South Dakota. During that time, I have

received additional training in collecting, preserving and analyzing evidence stored in different digital formats. The following is a list of specialized training I have received in conducting digital investigations and digital forensic examinations:

- Peer-to-Peer Computer Investigations
- Access Data BootCamp
- ICAC Unit Supervisor
- Internet Forensics
- Windows 7 Forensics
- Internet Relay Chat
- MAC Forensics
- Basic Data Recovery and Acquisition
- Intermediate Data Recovery and Acquisition
- Secure Techniques for On-Scene Preview
- Identification and Seizure of Electronic Evidence
- ICAC Ares
- Child Exploitation
- ICAC eMule Investigations
- Child Pornography the Ultimate Tool to Rescue Children
- ICAC BitTorrent Investigations
- Identification of Child Sex Trafficking
- NUIX Basic
- Cybertip Management
- 2014 Techno Security Conference
- 2015 National ICAC Conference
- 2015 Crimes Against Children Conference
- Android Open Source Forensics – Epyx Forensics
- Online Ads Investigations
- Undercover Chat Investigations
- Forensics Investigations with NetClean/Griffeye Analyze
- 2016 National ICAC Conference
- 2016 State of the States Cyber Crime Conference
- 2016 Florida ICAC Symposium
- 2017 Association of State Criminal Investigative Agencies
- 2017 Sex Offender Registry Conference
- 2017 South Dakota Technology Teachers Conference
- 2017 US Attorney's Office Law Enforcement Coordinating Committee Training Seminar
- 2017 South Dakota Society for Technology in Education Conference
- Cellebrite Training

- 2018 Appointed as a Special Deputy US Marshall under the Federal Bureau of Investigation
- Co-Chair National Internet Crimes Against Child Emerging Technology Committee
- South Dakota Center for the Prevention of Child Maltreatment Advisory Board Member.
- Griffeye Analyze DI Training.

3. In addition to the training I have received, I have presented to numerous professional groups and organizations and have testified as an expert on numerous occasions in US District Court, US Magistrate Court, and South Dakota Circuit Court.

4. I have investigated and assisted in the investigation of cases involving the possession, receipt, and distribution of child pornography in violation of federal law to include United States Statues 18 U.S.C. §§ 2251, 2252 and 2252A. During my law enforcement-career, I have become familiar with the *modus operandi* of persons involved in the illegal production, distribution and possession of child pornography and those who engage in enticement of minors using the internet. Based on my experience and training, I am knowledgeable of the various means utilized by individuals who illegally produce, distribute, receive and possess child pornography.

5. I have been informed that 18 U.S.C. §§ 2251, 2252, and 2252A prohibit the manufacture, distribution, receipt, and possession of child pornography.

6. The facts set forth in this affidavit are based on my personal knowledge, knowledge obtained from other individuals, including other law enforcement officers, interviews of persons with knowledge, my review of

documents, interview reports and computer records related to this investigation, communications with others who have personal knowledge of the events and circumstances described herein, and information gained through my training and experience. This affidavit contains information necessary to support probable cause for this application and does not contain every material fact that I have learned during the course of this investigation; however, I have not withheld information known to me that would tend to negate probable cause has been withheld from this affidavit.

**ITEMS TO BE SEARCHED FOR AND SEIZED:**

7. This affidavit is submitted in support of an application for a search warrant for the contents of Google Cybertip #62781662, hereafter also referred to as SUBJECT CYBERTIP, currently in the possession of ICAC, for contraband and evidence, fruits, and instrumentalities of violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt, and possession of child pornography).

**BACKGROUND ON CHILD PORNOGRAPHY AND CYBERTIPS**

8. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

- a. PhotoDNA is a process where a photograph is scanned by converting images into a grayscale format, creating a grid and assigning a numerical value to each tiny square. Those numerical values represent the “hash” of an image, or its “PhotoDNA signature.” The program protects user privacy in that

it doesn't look at images or scan photos; it simply matches a numerical hash against a database of known illegal images. A hash is an alphanumeric value assigned to an image based off a mathematical algorithm run against the data making up the file itself. This process has proven to be a reliable method of confirming like images.

- b. Electronic Service Providers (ESP's) report potential Child Exploitation they find on their servers to NCMEC. ESP's, as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.
- c. "Internet Protocol address" or "IP address," as used herein, refers to a unique number used by a computer to access the Internet. IP addresses can be "dynamic," meaning that the ISP assigns a different unique number to a computer every time it accesses the Internet. IP addresses might also be "static," if an ISP assigns a user's computer a particular IP address that is used each time the computer accesses the Internet.
- d. Offenders commonly trade Child Exploitation Material through email.
- e. "Sexually explicit conduct," as defined in 18 U.S.C. § 2256(2),



means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person.

- f. "Visual depiction," as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.
- g. Computers and digital technology have dramatically changed the way in which individuals interested in child pornography interact with each other. Computers serve many functions for persons who exploit children online; they serve as a mechanism for meeting child-victims and communicate with them; they serve as a mechanism to get images of the children and send images of themselves; computers serve as the manner in which persons who exploit children online can meet one another and compare notes.
- h. Persons, who exploit children online, can now transfer printed photographs into a computer-readable format with a device known as a scanner and then distribute the images using email,

like Gmail and Yahoo! Inc. Furthermore, with the advent of digital cameras and smartphones with cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a computer by simply connecting the camera or smartphone to the computer. In the last ten years, the resolution of pictures taken by digital cameras and smartphones has increased dramatically, meaning that such pictures have become sharper and crisper. Photos taken on a digital camera or smartphone may be stored on a removable memory card in the camera or smartphone. These memory cards often store up to 32 gigabytes of data, which provides enough space to store thousands of high-resolution photographs. Video camcorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The user can easily transfer video files from the camcorder to a computer.

- i. A device known as a modem allows any computer to connect to another computer with telephone, cable, or wireless connection. People can make electronic contact to literally millions of computers around the world. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of



child pornography. Persons can transfer child pornography via electronic mail or through file transfer protocols (FTPs) to anyone with access to a computer and modem. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., “instant messaging”), and easy access to the Internet, the computer is a preferred method of distribution and receipt of child pornographic materials.

- j. The Internet affords individuals several different venues for meeting and exploiting children in a relatively secure and anonymous fashion.
- k. Individuals also use online resources to exploit children, including services offered by Internet Portals such as Gmail and Hotmail, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any computer with access to the Internet. Even in cases where a user utilizes online storage is, evidence of child pornography can be found on the user’s computer or external media in most cases.

9. Based on the ruling in *United States v. Ackerman*, 831 F.3d 1292 (10th Cir. 2016), the Department of Justice recommends when the content of a Cybertip has not been viewed and confirmed to be child pornography by

members of the ESP or NCMEC that law enforcement seek a search warrant. I submit this affidavit in support of the search warrant for the SUBJECT CYBERTIP based on this legal guidance.

**PROBABLE CAUSE**

10. On January 14, 2020, Google, Inc. filed a Cybertip with the National Center for Missing and Exploited Children (NCMEC). NCMEC assigned this Cybertip the number #62781662. NCMEC subsequently sent the Cybertip to me on March 2, 2020.

11. In the Cybertip, Google, Inc. indicated they located an image that was stored in the Google Mail Infrastructure as well as the Google Drive Infrastructure. There were two images uploaded with this account that Google identified as being child pornography through a process called hash match. The program protects user privacy in that it does not look at images or scan photos; it simply matches a numerical hash against a database of known illegal images. A hash is an alphanumeric value assigned to an image based off a mathematical algorithm run against the data making up the file itself. This process has proven to be a reliable method of confirming like images.

12. The suspected child pornography images were uploaded in the Google, Inc. account associated with the email address: [wakiyan777@gmail.com](mailto:wakiyan777@gmail.com). Google, Inc. provided the images to NCMEC, however the images were not viewed or confirmed to be contraband by either Google, Inc. or NCMEC.

13. NCMEC geo-located the IP Address provided by Google, Inc. and found the IP Address belonged to Golden West Telecommunications and resolved to Kyle, SD.

14. Based on the information provided above I believe probable cause exists to view the image contained in Cybertip #62781662.

**CHARACTERISTICS COMMON TO INDIVIDUALS WHO HAVE A SEXUAL  
INTEREST IN CHILDREN AND/OR WHO RECEIVE AND/OR POSSESS  
CHILD PORNOGRAPHY**

15. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who have a sexual interest in children and/or receive, or possess images of child pornography:

- a. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.
- b. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or

images of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography almost always possess and maintain their hard copies of child pornographic material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home or some other secure location. Individuals who have a sexual interest in children or images of children often retain pictures, films, photographs, negatives, magazines, correspondence, books, tape recordings, mailing lists, child erotica, and videotapes for many years.

d. Likewise, individuals who have a sexual interest in children and/or receive, or possess images of child pornography often maintain their child pornography images in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area. The user often maintains these child pornography images for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly.

e. Individuals who have a sexual interest in children and/or receive,

or possess images of child pornography also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Individuals who have a sexual interest in children and/or receive, or possess images of child pornography prefer not to be without their child pornography for any prolonged time-period. Law enforcement officers involved in the investigation of child pornography throughout the world have documented this behavior. Thus, even if the unknown user uses a portable device (such as a mobile cell phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found within the SUBJECT ACCOUNT.

#### **JURISDICTION**

16. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711(3). 18 U.S.C. §§ 2703(a), (b)(1)(A) & (c)(1)(A). Specifically, this Court is a "district court of the United States (including a magistrate judge of such court)" that "has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

#### **LIMIT ON SCOPE OF SEARCH**

17. I submit that if during the search, agents find evidence of crimes

not set forth in this affidavit, another agent or I will seek a separate warrant.

**REQUEST FOR SEALING OF MATTER**

18. I request that the Court order sealing this case until further order of the Court. The documents filed in the case discuss an ongoing criminal investigation that is neither public nor known to all the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to flee, destroy or tamper with evidence, change patterns of behavior, notify confederates, or otherwise seriously jeopardize the investigation.

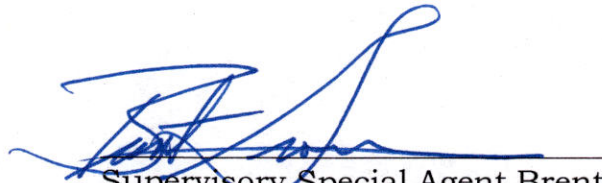
**CONCLUSION**

19. Based on my training and experience, and the facts as set forth in this affidavit, there is probable cause to believe that there exists evidence of a crime, contraband, instrumentalities, and/or fruits of violations of criminal laws as specified herein, including identification of the person who used the Google account to download the images of child pornography contained in the SUBJECT CYBERTIP. The facts outlined above show that the Google account associated with the SUBJECT CYBERTIP, has been used for the exploitation of children using the internet including violations of 18 U.S.C. §§ 2251, 2252, and 2252A (production, receipt and possession of child pornography). There is probable cause to believe that the unidentified user received and distributed child pornography with other unknown Google users, and thereby violated the aforementioned statutes in the District of South Dakota and elsewhere.



The Cybertip containing downloads from this account is the subject of this warrant affidavit.

Dated: 3/23/20




Supervisory Special Agent Brent Gromer  
SD DCI and SD ICAC Commander  
FBI TFO

SUBSCRIBED and SWORN to

du in my presence  
\_\_\_\_\_ by reliable electronic means

this 23rd day of March, 2020.



DANETA WOLLMANN  
U.S. MAGISTRATE JUDGE



**ATTACHMENT A**  
**Property to Be Searched**

The contents of Google Cybertip #62781662

**ATTACHMENT B**

**ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of Title 18, United States Code, Sections 2251, 2252 and 2252A and 2422(b): the contents of Google Cybertip #62781662.

## UNITED STATES DISTRICT COURT

for the  
District of South DakotaIn the Matter of the Search of:  
Google Cybertip #62781662) Case No. 5:20-mj-69  
)  
)  
)  
)  
)

## SEARCH AND SEIZURE WARRANT

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search of the following person or property located in the District of South Dakota (identify the person or describe the property to be searched and give its location):

See **ATTACHMENT A**, attached hereto and incorporated by reference

I find that the affidavit, or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

Evidence of a crime in violation of 18 U.S.C. §§ 2251, 2252, and 2252A, as described in **ATTACHMENT B**, attached hereto and incorporated by reference.

I find that the affidavit, or any recorded testimony, establishes probable cause to search and seize the person or property.

**YOU ARE COMMANDED** to execute this warrant on or before April 6, 2020 (not to exceed 14 days)

☐ in the daytime 6:00 a.m. to 10 p.m. ☒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Daneta Wollmann.  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for \_\_\_\_\_ days (not to exceed 30). ☐ until, the facts justifying, the later specific date of \_\_\_\_\_.

☐ I find that good cause has been established to authorize the officer executing this warrant to not provide notice prior to the execution of the search warrant, i.e., "no knock".

Date and time issued: 3-23-2020 10:05am  
Judge's signatureCity and state: Rapid City, SDDaneta Wollmann, U.S. Magistrate  
Printed name and title

cc: AUSA Collins, and Agent

Return		
Case No.: 5:20-mj-69	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name of any person(s) seized:                    		
Certification		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <p>Date: _____</p> <p>_____ <i>Executing officer's signature</i></p> <p>_____ <i>Printed name and title</i></p>		